UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA

NIDA SAMSON, Individually and On Behalf of All Others Similarly Situated, Plaintiff, v. EQUIFAX, INC., Defendant.	**Civil Action No.** CLASS ACTION COMPLAINT **JURY TRIAL DEMANDED**

Plaintiff, Nida Samson ("Plaintiff"), on behalf of herself and others similarly situated, brings this class action against Equifax, Inc. ("Equifax" or the "Company"). Plaintiff makes the following allegations, except as to allegations specifically pertaining to Plaintiff, upon information and belief based upon, *inter alia*, the investigation of counsel and review of public documents.

NATURE OF THE ACTION

1. This is a class action on behalf of the 143 million individuals whose sensitive personal identifying information was compromised in a cybersecurity breach of Equifax, which was announced on September 7, 2017 (the "Equifax Breach").

2. According to Equifax's public announcement of the Equifax Breach, the compromised information includes Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. Also, hackers accessed credit card numbers and certain dispute documents with personal identifying information for some consumers.

3. Equifax failed to adequately protect consumers' sensitive personal identifying information. Lack of proper safeguards provided a means for unauthorized intruders to breach Equifax's computer network and steal sensitive personal identifying information.

4. Armed with this sensitive personal identifying information, hackers can commit a variety of crimes including, among other things, taking out loans in another person's name; opening new financial accounts in another person's name; using the victim's information to obtain government benefits; filing a fraudulent tax return using the victim's information to obtain a tax refund; obtaining a driver's license or identification card in the victim's name but with another person's picture; or giving false information to police during an arrest.

5. As a result of the Equifax Breach, Plaintiff and Class members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class members must now and in the future closely monitor their financial accounts to guard against identity theft. Plaintiff and Class members may be faced with fraudulently incurred debt. Plaintiff and Class members may also incur out of pocket costs for, among other things, obtaining credit reports, credit freezes, or other protective measures to deter or detect identity theft.

6. Plaintiff seeks to remedy these harms on behalf of themselves and all similarly-situated individuals and entities whose sensitive personal identifying information was accessed during the Equifax Breach.

7. Plaintiff seeks remedies including but not limited to reimbursement of out-of-pocket losses, further credit monitoring services with accompanying identity theft insurance, and improved data security.

PARTIES

8. Plaintiff Nida Samson resides and is a citizen of the state of Pennsylvania.

9. In response to Equifax's announcement of the Equifax Breach, Plaintiff visited the Equifax Breach Website (defined below) on September 7, 2017 and confirmed that her sensitive personal identifying information had been compromised by the Equifax Breach. Despite being affected by the Equifax Breach, Plaintiff was not eligible for enrollment in credit monitoring and identity theft protection, according to the Equifax Breach Website, until September 13, 2017.

10. The Equifax Breach Website instructed Plaintiff:

> On or after your enrollment date, please return to faq.trustedidpremier.com and click the link to continue through the enrollment process.

11. Defendant Equifax, Inc. is incorporated in the state of Georgia. Its headquarters and principal place of business are located at 1550 Peachtree Street, NW, Atlanta, GA 30309.

12. Equifax describes itself as a "global information solutions company." The company organizes, assimilates and analyzes data on more than 820 million consumers …" and among Equifax's business lines are "consumer and commercial credit reporting and scoring."[1]

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). If a class is certified in this action, the amount in controversy will exceed $5,000,000.00, exclusive of interest and costs. At least one member of the proposed class is a citizen of a state different from Equifax. Greater than two-thirds of the members of the proposed class are citizens of states other than Georgia.

[1] https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628

14. This Court has personal jurisdiction over Equifax, because Equifax is incorporated in, and its headquarters and principal place of business are located within, Georgia.

15. Venue is also proper within this District because, pursuant to 28 U.S.C. § 1391(b)(1) & (c)(1), Equifax is deemed to reside in this District since it is subject to personal jurisdiction in this District. Finally, venue is proper in this District because a substantial part of the events or omissions giving rise to the claim occurred in this District.

SUBSTANTIVE ALLEGATIONS

THE EQUIFAX BREACH

16. According to a statement released by Equifax on September 7, 2017:

> Equifax, Inc. [] today announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers… The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed.[2]

17. Equifax briefly explained that, "[c]riminals exploited a U.S. website application vulnerability to gain access to certain files." Equifax also disclosed that "unauthorized access occurred from mid-May through July 2017."[3]

18. According to Equifax, it did not discover the Equifax Breach until July 29, 2017. And, Equifax delayed its public announcement of Equifax Breach until September 7, 2017.[4]

19. In describing the breach, Equifax's Chairman and Chief Executive Office, Richard F. Smith, released the following statement:

> This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes …. We pride ourselves

[2] https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628
[3] *Id.*
[4] *Id.*

> on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations. We also are focused on consumer protection and have developed a comprehensive portfolio of services to support all U.S. consumers, regardless of whether they were impacted by this incident.[5]

20. Notably, it has also been reported that three Equifax executives sold nearly $2 million in shares in the company, days after the Equifax Breach was discovered (but before it was announced publicly).[6]

21. Equifax failed to adopt adequate protective measures to prevent hackers' exploitation of a vulnerability in a website application and failed to ensure that consumers' sensitive personal identifying information would not be improperly accessed.

22. Once Equifax's systems had been compromised, Equifax failed to timely discover the breach and implement adequate remedial measures to secure consumers' sensitive personal identifying information.

23. As a result of Equifax's inadequate measures, sensitive personal identifying information was obtained from Equifax's computer network over a period of approximately six weeks before detection.

24. Moreover, Equifax failed to timely inform consumers of the Equifax Breach – waiting over a month after it was discovered before making its public announcement.

EQUIFAX'S POST-BREACH ACTIONS ARE INADEQUATE

25. In the wake of the breach, Equifax has established a dedicated website – https://www.equifaxsecurity2017.com/ (the "Equifax Breach Website") – which allows consumers to determine if they were impacted by the Equifax Breach. The website also allows

[5] *Id.*
[6] https://www.cnbc.com/2017/09/07/credit-reporting-firm-equifax-says-cybersecurity-incident-could-potentially-affect-143-million-us-consumers.html

affected consumers to sign up for credit monitoring and theft protection through TrustedID Premier, however the enrollment period for such services ends on November 21, 2017.[7]

26. There have been reports, however, that the Equifax Breach Website has not functioned for potentially affected consumers.[8]

27. Aside from this issue, Equifax has taken no steps to date to notify consumers of the cybersecurity breach and the potential theft of their sensitive personal identifying information, aside from issuing its press release and establishing a website.[9]

28. Equifax claims that it will send direct mail notices of the cybersecurity breach to those consumers whose credit card numbers or dispute documents with personal identifying information have been stolen. Equifax, however, has no plans to independently notify the consumers whose sensitive personal identifying information – names, Social Security numbers, birth dates, addresses and driver's license numbers – was compromised. [10]

29. Even consumers who are aware of the Equifax Breach, have been unable to secure immediate protections for their stolen data.

30. Plaintiff confirmed that her sensitive personal identifying information was compromised on the Equifax Breach Website, however Plaintiff was informed that credit monitoring and identity theft protection would not be available to her until September 11, 2017.

31. Moreover, even before it starts, Equifax has recognized the limitations in the credit monitoring and identity theft protection being offered to consumers.

---

[7] https://www.equifaxsecurity2017.com/enroll/

[8] *See, e.g.,* http://www.businessinsider.com/equifax-data-breach-site-check-angry-response-2017-9; http://www.marketwatch.com/story/after-huge-data-breach-equifax-not-telling-all-customers-if-they-are-affected-2017-09-07

[9] https://www.equifaxsecurity2017.com/frequently-asked-questions/

[10] https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628

32. For example, with respect to "Social Security Number Monitoring," Equifax admits that "there is no guarantee that Identity Protection provided by Equifax is able to locate and search every possible internet site where consumers' personal information is at risk of being traded."[11]

33. With respect to identity theft insurance, Equifax recognizes that "[c]overage may not be available in all jurisdictions."[12]

34. Further, the Terms of Use for TrustedID Premier – the Equifax entity through which Equifax is offering credit monitoring and identity theft protection – include arbitration and class action waiver clauses.[13]

35. Also notable, Equifax's general Terms of Use state: "[w]e do not offer, provide, or furnish any Products, or any advice, counseling, or assistance, for the express or implied purpose of improving Your credit record, credit history, or credit rating."[14]

36. The New York State Office of the Attorney General opened an investigation into the Equifax breach on September 8, 2017. Attorney General Eric T. Schneiderman issued a consumer alert related to the breach and sent Equifax a letter seeking additional information.[15]

CLASS ACTION ALLEGATIONS

37. Plaintiff brings this class action pursuant to Fed. R. Civ. P. 23 on behalf of itself and all others similarly situated (the "Class"). The Class is defined as:

> All individuals and entities in the United States whose personal identifying information was accessed in the cybersecurity breach announced by Equifax on September 7, 2017.

[11] https://www.equifaxsecurity2017.com/trustedid-premier/
[12] *Id.*
[13] https://www.trustedid.com/serviceterms.php
[14] http://www.equifax.com/terms/
[15] https://ag.ny.gov/press-release/ag-schneiderman-launches-formal-investigation-equifax-breach-issues-consumer-alert

38. Excluded from the Class are Equifax; any parent, subsidiary, or affiliate of Equifax or any employees, officers, or directors of Equifax; legal representatives, successors, or assigns of Equifax; and any justice, judge, or magistrate judge of the United States who may hear the case, and all persons related to any such judicial officer, as defined in 28 U.S.C. § 455(b).

39. Upon information and belief, the proposed Class consists of millions of geographically dispersed members, the joinder of whom in one action is impracticable. Disposition of the claims in a class action will provide substantial benefits to both the parties and the Court.

40. The rights of each member of the Class were violated in a similar fashion based upon Equifax's uniform wrongful actions and/or inaction.

41. The following questions of law and fact are common to each Class member and predominate over questions that may affect individual Class members:

A. whether Equifax engaged in the wrongful conduct alleged herein;

B. whether Equifax was negligent in collecting, storing, and/or safeguarding the sensitive personal identifying information of the Class members;

C. whether Equifax owed a duty to Plaintiff and Class members to adequately protect their personal information;

D. whether Equifax breached its duties to protect personal information of Plaintiff and Class members;

E. whether Equifax knew or should have known that its data security systems and processes were vulnerable to attack;

F. whether Equifax's conduct proximately caused damages to Plaintiff and Class members;

G. whether Plaintiff and Class members are entitled to equitable relief including injunctive relief; and

H. whether the Class members are entitled to compensation, monetary damages, and/or any other services or corrective measures from Equifax, and, if so, the nature and amount of any such relief.

42. Plaintiff's claims are typical of the claims of the Class in that Plaintiff, like all Class members, had her sensitive personal identifying information compromised in the data breach.

43. Plaintiff is committed to the vigorous prosecution of this action and will fairly and adequately represent and protect the interests of the proposed Class. Plaintiff has no interests that are antagonistic to and/or that conflict with the interests of other putative Class members.

44. Plaintiff has retained counsel competent and experienced in the prosecution of complex class action litigation.

45. The members of the proposed Class are readily ascertainable.

46. A class action is superior to all other available methods for the fair and efficient adjudication of the claims of the Class and the Class members. Plaintiff and the Class members have suffered (and continue to suffer) irreparable harm as a result of Equifax's conduct. The damages suffered by some of the Class members may be relatively small, preventing those Class members from seeking redress on an individual basis for the wrongs alleged herein. Absent a class action, many Class members who suffered damages as a result of the cybersecurity breach of Equifax will not be adequately compensated.

47. Prosecuting separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for

Equifax. Additionally, adjudications with respect to individual Class members, such as adjudication as to injunctive relief, as a practical matter, would be dispositive of the interests of the other Class members not parties to the individual adjudications or would substantially impair or impede their ability to protect their interests.

COUNT ONE

NEGLIGENCE

48. Plaintiff realleges and incorporates all allegations set forth in previous paragraphs as if fully set forth herein.

49. Upon coming into possession of the private, sensitive personal information of Plaintiff's and the Class members, Equifax had (and continues to have) a duty to exercise reasonable care in safeguarding and protecting the information from being compromised and/or stolen. Equifax's duty arises from the common law, in part because it was reasonably foreseeable to Equifax that a breach of security was likely to occur under the circumstances and would cause damages to the Class as alleged herein.

50. Equifax also had a duty to timely disclose to Plaintiff and Class members that the Equifax Breach had occurred and that the sensitive personal identifying information of the Class members – particularly Social Security numbers, dates of birth, addresses, driver's license numbers, and in some cases sensitive financial information, such as credit card numbers and dispute documents – had been, or was reasonably believed to be, compromised. Such duty also arises under the common law because it was reasonably foreseeable to Equifax that a breach of security was likely to occur under the circumstances and would cause damages to the Class as alleged herein.

51. Equifax, by and through its above negligent acts and/or omissions, further breached its duties to the Class members by failing to timely disclose to Plaintiff and Class members that the Equifax Breach had occurred and that the sensitive personal identifying information of Plaintiff and the Class members had been compromised. Instead, Equifax breached its duty by staying silent about the Equifax Breach for over a month after it was discovered.

52. Equifax also had a duty to put into place internal policies and procedures designed to detect and prevent the unauthorized dissemination of the Plaintiff and Class members' sensitive personal identifying information. Such duty also arises under the common law because it was reasonably foreseeable to Equifax that a breach of security was likely to occur under the circumstances and would cause damages to the Class as alleged herein.

53. Equifax, by and through its above negligent acts and/or omissions, unlawfully breach its duties to the Class members by, *inter alia*, failing to exercise reasonable care in protecting and safeguarding the Class members' sensitive personal identifying information within its possession, custody, and control.

54. But for Equifax's negligent and wrongful breach of the duties it owed (and continues to owe) to Plaintiff and the Class members and the cybersecurity breach would not have occurred, Plaintiff's and the Class members' sensitive personal identifying information would never have been compromised.

55. The Equifax Breach and the above-described substantial injuries suffered by Plaintiff and the Class members as a direct and proximate result of the breach were reasonably foreseeable consequences of Equifax's negligence.

COUNT TWO

NEGLIGENCE PER SE

56. Plaintiff realleges and incorporates all allegations set forth in previous paragraphs as if fully set forth herein.

57. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair…practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect sensitive personal identifying information.

58. In 2007, the FTC published guidelines which establish reasonable data security practices for businesses. The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vender-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

59. The FTC also has published a document entitled "FTC Facts for Business" which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

60. Further, the FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

61. By failing to have reasonable data security measures in place, Equifax engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

62. Equifax's violation of Section 5 of the FTC Act constitutes negligence *per se.*

63. The Equifax Breach and the above-described substantial injuries suffered by Plaintiff and the Class members as a direct and proximate result of the breach were reasonably foreseeable consequences of Equifax's negligence *per se*.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that the Court certify this action as a class action, with Plaintiff as class representative and the undersigned counsel as class counsel, and enter an order of judgment against Equifax in favor of the Class that, *inter alia*:

A. awards actual damages to fully compensate the Class for losses sustained as a direct, proximate, and/or producing cause of Equifax's unlawful conduct;

B. awards pre-judgment and post-judgment interest at the maximum allowable rates;

C. appropriate injunctive and equitable relief;

D. awards reasonable attorneys' fees and costs; and

E. orders any further relief that this Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury to the extent permitted by law.

Dated: September 8, 2017

/s/ Lisa L. Heller
ROBBINS ROSS ALLOY BELINFANTE LITTLEFIELD LLC
Lisa L. Heller
999 Peachtree Street, N.E. Suite 1120
Atlanta, GA 30309
Tel: (678) 701-9381
Fax: (404) 856-3250

KESSLER TOPAZ MELTZER & CHECK LLP
Naumon A. Amjed
Joshua D'Ancona
Ethan J. Barlieb
Meredith L. Lambert
280 King of Prussia Road
Radnor, PA 19087
Tel: (610) 667-7706
Fax: (610) 667-7056

COOPER & KIRK, PLLC
David H. Thompson
Davis Cooper
1523 New Hampshire Avenue, N.W.
Washington, D.C. 20036
Tel: (202) 220-9600
Fax: (202) 220-9601

Attorneys for Plaintiff Nida Samson